UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/083,010	02/26/2002	Matthew Charles Priestley	MS190438.1	4314

27195 7590 08/10/2007

AMIN. TUROCY & CALVIN, LLP
24TH FLOOR, NATIONAL CITY CENTER
1900 EAST NINTH STREET
CLEVELAND, OH 44114

EXAMINER	
ABEDIN, SHANTO	

ART UNIT	PAPER NUMBER
2136	

MAIL DATE	DELIVERY MODE
08/10/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/083,010	PRIESTLEY ET AL.	
	Examiner	Art Unit	
	Shanto M Z Abedin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *03* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 May 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-18,20-29 and 31-33* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-18,20-29 and 31-33* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the **APPEAL BRIEF** filed on 05/07/2007, and this office action is made **NON-FINAL.**

2. Claims 1, 3-18, 20-29 and 31-33 are currently presented for the examination.

3. Claims 1, 3-18, 20-29 and 31-33 have been rejected.

4. The examiner notes, upon further examination, new grounds of 35 USC 101 and 35 USC 112 type rejections are found, and addressed in this office action (Please see below for detail).

Response to Arguments

5. The applicant's arguments regarding previous 35 USC 103 type rejections are fully considered, however, they are moot in view of new grounds of rejection (Please see below for detail).

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

6. ***Claims 1, 3-16, 27-29, 31 and 33*** are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claims 1, 3-16 and 31-32, they are directed to a system, however, the language of the claim(s) raises a question whether the claim is directed merely to an abstract idea, or software only implemented system that is not tied to an environment or machine or hardware. Although preamble of the claims recite a computer implemented system, claimed limitations fail to disclose any computer or hardware or machine, instead, they merely discloses software implemented element (such as service), or data structures (such as a wrapper or a pass-phrase) along with their intended uses. Therefore, invention can be implemented by software alone, or directed to non-statutory subject matter. MPEP 2106.01 [R-5].

Regarding claim 27, they are directed to a system, however, the language of the claim(s) raises a question whether the claim is directed merely to an abstract idea, or software only implemented system that is not tied to an environment or machine or hardware. Although claim language incorporate computer implemented means, the specification fails to disclose such computer implemented means as hardware element or machines or computers. Such computer implemented means could be executables or software or program. Therefore, invention can be implemented by software alone, or directed to non-statutory subject matter. MPEP 2106.01 [R-5].

Regarding claims 28-29 and 33, they are directed to a compute readable medium merely storing non functional descriptive materials, or data structures, therefore, being non-statutory. MPEP 2106.01 [R-5].

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 28-29 and 33 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claims 28-29, they recite the limitations such as "first data packet comprising a password component ...and a wrapper field...a second data packet comprising a passphrase " However, specification fails to disclose first data packet comprising a password component and a wrapper field, rather Fig 1 of the specification only suggests at best, storing and signaling a wrapped credential/ password as first data packet, and a passphrase as second data packet. In short, specification fails to disclose storing a wrapper field itself, and a (unwrapped) password component as a part of first data packet.

Regarding claim 33, it recites the limitations such as "a first field...a second field...a third field containing a wrapper". However, specification fails to disclose such inter-related first, second, third data field stored as a single data structure, rather Fig 1 shows at best storing wrapped credential/ password, and passphrase together. In short, specification fails to disclose a seperate wrapper and a (unwrapped) credential as a component of a data structure, rather only discloses storing a wrapped credential/password together with passphrase. Therefore, at the time of invention, one skilled in the art would not be able to, or would not feel any need to produce a data structure comprising wrapper and (unwrapped!) credential and passphrase, rather only be able to produce a data structure comprising a wrapped credential and passphrase.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1, 6-15 and 17 are rejected under 35 USC 103 (a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300).

Regarding claim 1, Brainard discloses a computer implemented system for processing credentials, comprising the following computer executable components:

a wrapper (Page 3, Section 2.2 to Page 4 Section 2.2; Page 7, Table 2; (unlocking)key used to encrypt PSD or PAC or EAR or password) that packages credentials associated with resources of a service (Page 3, Section 2.2 to Page 4 Section 2.2; Page 6, Section 3.5; encrypted passwords; Page 7, Table 2; locked or protected PSD or EAR) ; and

the credentials employed to facilitate access to the resources of the service (Page 3, Section 2.2 to Page 4 Section 2.2).

Brainard fails to disclose

a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key, the pass-phrase employed to facilitate access to the credentials, and the pass-phrase distributed separately from the credentials.

However, Hypponen discloses a pass-phrase employed in connection with generation of the wrapper via a cryptographic wrapping key (Col 3, lines 35-65; generating cryptographic key from passphrase), the pass-phrase employed to facilitate access to the credentials (Col 3, lines 15-25; passphrase is employed to encrypt/ decrypt password/ credential in case of password based symmetric cryptographic key).

Modified Brainard-Hypponen system fails to disclose

the pass-phrase distributed separately from the credentials.

However, Bathrick et al discloses the pass phrase distributed separately from the credentials (Col 2, lines 33-40, 64-67; Claim 1; distributing keying and certificate material separately; the examiner interprets keying material as passphrase, and certificate material as credential).

Hypponen , Bathrick et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Hypponen with Brainard for employing pass-phrase in connection with generation of the wrapper via a cryptographic wrapping key in order to provide a pass-phase based protection, and to combine teachings of Bathrick et al with modified Hypponen - Brainard system to provide further protection against unauthorized access to the passphrase and the credential.

Regarding claim 6, Brainard discloses the system of claim 1, further comprising one or more partners to request access to the resources (Section 1.2; agents).

Regarding claim 7, Brainard discloses the system of claim 6, at least one of the partners includes a credential store to manage the credentials (Section 2.2; generating and storing credentials).

Regarding claims 8 and 9, these limitations are already addressed in terms of rejecting claims 1, 6-7.

Regarding claims 10-12, Brainard discloses use of that pass phrase over a SSL connection or in a VPN environment (Page 6, Col 1, step 5, application server, SSL connection); and issuing an Electronic License Certificate (Section 3.1; PAC).

Regarding claims 13-14, Brainard teaches a platform provisioning service, or such service being associated with a partner including a service provider and tenant (Fig 5, PAC; SecurSight authentication service; system consist of manager, desktop, and application server; Brainard's enterprise network resources and applications imply capability of performing billing, financial, or accounting functions) .

Regarding claims 15 and 17, these limitations are already addressed in terms of rejecting claims 1, 6-7 and 13-14.

9. Claim 16 is rejected under 35 USC 103 (a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300) further in view of Kay et al (US 6993555B2).

Regarding claim 16, Kay et al discloses at least one of the platform provisioning service and the partner maintain an account to process the credentials, the at least one of the platform provisioning service and the partner employ a Universal Resource Locator (URL) to present the credentials to the account (Col 11, starts at line 64; URL containing authentication information).

Kay et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it

would have been obvious to a person of ordinary skill in the art to combine the teaching of Kay et al with modified Brainard method to design a method employing a Universal Resource Locator (URL) to present the credentials to the account in order to provide an access request with the access credentials.

10. Claims 3-5 are rejected under 35 USC 103 (a) as being unpatentable over Brainard (SecurSight: An Architecture for Secure Information) in view of Hypponen (US 6986050 B2) further in view of Bathrick et al (US 5825300) further in view of Rahman et al (US 7114080 B2) .

Regarding claim 3, Rahman et al discloses the credentials providing stronger encryption than the pass-phrase (Col 3, starts at line 4; Col 7, starts at line 50; using strong password; the examiner interprets such strong password usually has stronger encryption than an alphanumeric passphrase).

Rahman et al and Brainard are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Rahman et al with modified Brainard method to design a method wherein credentials providing stronger encryption than the pass-phrase in order to provide transferring of a strong credential.

Regarding claim 4, Rahman et al discloses the credentials providing greater than 100 bits of encryption (Col 3, starts at line 4; Col 7, starts at line 50; using strong password).

Regarding claim 5, Hypponen discloses the pass-phase having human-readable alpha-numeric characteristics. (Col 1, lines 40-65; passphrases)

11. Claim 18 and 20 are rejected under 35 USC 103 (a) as being unpatentable over Epstein et al (US 2002/0124064 A1) in view of Hardy et al (US 5222135) further in view of Bathrick et al (US 5825300).

Regarding claim 18, Epstein et al discloses a a method to facilitate a security connection between entities, comprising:

generating a strong password (Fig 6A; Par [0055], [0062], [0111]; one-time passwords);

generating a pass-phrase (Fig 6A; Par [0029], [0111]; passphrase);

wrapping the password cryptographically via the pass-phrase (Par [0029]; Claims 25, 68; password encoded in passphrase);

Epstein et al fails to disclose

storing the wrapped password in an executable; and

transmitting the executable and the pass-phrase to a system via different communications mediums.

However, Hardy et al discloses storing the wrapped password in an executable (Col 4, starts at line 32; Claim 12; storing encrypted password...later in executable form);

Modified Hardy et al - Epstein et al system fails to disclose

transmitting the executable and the pass-phrase to a system via different communications mediums.

However, Bathrick et al discloses transmitting the executable and the pass-phrase to a system via different communications mediums (Col 2, lines 33-40, 64-67; Claim 1; distributing keying material, and certificate material separately).

Hardy et al, Bathrick et al and Epstein et al are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Hardy et al with Epstein et al for storing the wrapped password in an executable to provide with executable password file and to combine teachings of Bathrick et al with modified Hardy et al-Epstein et al system to provide further protection against unauthorized access to the passphrase and the credential.

Regarding claim 20, Epstein et al discloses employing the pass-phrase to unlock the strong password stored in the executable, the strong password employed to establish a trust relationship with an entity (Par [0029]; Claims 25, 68; password encoded in passphrase).

12. Claims 21-26 are rejected under 35 USC 103 (a) as being unpatentable over Epstein et al (US 2002/0124064 A1) in view of Hardy et al (US 5222135) further in view of Bathrick et al (US 5825300) further in view of Brainard (SecurSight: An Architecture for Secure Information).

Regarding claims 21- 22, Brainard teaches a method comprising at least one of:

Verifying an SSL certificate (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service)[Brainard teaches an application access agent and a certificate validation service to validate SSL certificates];

Requesting a Universal Resource Locator (URL) from a listener(Section 2.4: Comparison with other authenticators)[Brainard teaches obtaining web browser based credentials which essentially refers to use of an URL] ;

Presenting authentication credentials to a receiver (Section 3.3: Use of PACs by connect agent; Section 4.2: Certificate Validation Service) [Brainard teaches desktop presenting a certificate to be validated by the certificate validation service.];

Logging in a caller to an account (Section 3.1: PAC definition; Section 3.3: use of PACs by connect agents) [Brainard teaches a connect agent that initiates a client's access to an account after certificates are validated].

Brainard and Epstein et al are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of

Brainard with modified Epstein et al for utilizing SSL certificate and UrL to provide access request in order to provide proper request security.

Regarding claim 24, Brainard teaches the method comprising at least one of: setting up account privileges; designating account contacts; and verifying contacts (Page 7, Col 1, Table 2, EAR; access right).

Regarding claim 25 is rejected applied as above rejecting claim 24. Furthermore, Lee et al does not expressly discloses a method of verbally communicating the password. However, Bathrick et al discloses a method comprising verbally communicating the password (Claim 3; non electronic communication medium for keying material/ password).

Regarding claims 23 and 26, these limitations are already addressed in terms of rejecting claims 18, 22-23 and 25.

13. Claims 27-29 and 31-33 are rejected under 35 USC 103 (a) as being unpatentable over Rahman et al (US 7114080 B2) in view of Nemovicher (US 2002/0007453 A1).

Regarding claim 27, Rahman et al discloses a computer executable system to facilitate a security relationship between parties, comprising:

computer implemented means for generating a password (Col 3, starts at line 4; Col 7, starts at line 50; generating password);

computer implemented means for generating a package of credentials (Col 3, starts at line 4; Col 7, starts at line 50; encrypted combined credential);

Rahman et al fails to disclose computer implemented means for generating a pass-phrase; computer implemented means for storing the password [[in]] separate from the package; computer implemented means for locking the package with the pass-phrase; and computer implemented means for transmitting the package and the pass-phrase to a system via different communications mediums.

However, Nemoviche teaches computer implemented means for generating a pass-phrase (Par [0082], [0089]); computer implemented means for storing the password separate from the package (Par [0081]-[0082]); computer implemented means for locking the package with the pass-phrase (Par [0082], [0089]); and computer implemented means for transmitting the package and the pass-phrase to a system via different communications mediums (par [0089]).

Nemoviche further teaches computer implemented means for generating a package of credentials (Par [0082]);

Rahman et al and Nemovicher are analogous art because they are from the same field of endeavor of secure electronic data transmission and retrieval. At the time of

invention it would have been obvious to a person of ordinary skill in the art to combine the teaching of Nemovicher with Rahman et al to design a medium wherein a second data packet comprising: a pass-phrase employed to generate and unlock the wrapper field, and the pass-phrase distributed separately from the wrapper field in order to provide further protection against unauthorized access to the credentials.

Regarding claim 28, Rahman et al discloses a computer-readable medium having stored thereon a signal to communicate security data between at least two nodes, comprising:

a first data packet comprising: a password component employed to establish a trust relationship between at least two nodes (Col 3, starts at line 4; Col 7, starts at line 50; utilizing password for accessing network data).

a wrapper field employed to encapsulate the password, the wrapper field mediating access to the password (Col 3, starts at line 4; Col 7, starts at line 50; encrypting the strong password with key).

Rahman et al fails to disclose a second data packet comprising: a pass-phrase employed to generate and unlock the wrapper field, the pass-phrase distributed separately from the wrapper field.

However, Nemovicher discloses

a second data packet comprising: a pass-phrase employed to generate and unlock the wrapper field (Par [0082], [0089]; using a passphrase or password to generate the public or private key; opening package with the passphrase or password), the pass-phrase distributed

separately from the wrapper field (Par [0082], [0089]; Nemovicher teaches enablement of sending passphrase separately from the package (comprising the keys generated from the password or passphrase));

Nemovicher further discloses

a password component employed to establish a trust relationship between at least two nodes (Par [0082], [0089]; using password or passphrase to unlock the email package); and

a wrapper field employed to encapsulate the password, the wrapper field mediating access to the password (Par [0082], [0089]; locked package including encrypted password ; using a private/ public key (derived from the password or passphrase) to encode the package).

Regarding claim 29, Rahman et al discloses wrapper field being cryptographically weaker than the password (Col 3, starts at line 4; Col 7, starts at line 50; using strong password; the examiner interprets such encryption keys are weaker than the strong passwords).

Regarding claims 31-33, they recite the limitations similar to claims 27-29, therefore, they are rejected applying as above rejecting claims 27-29.

Conclusion

14. A shortened statutory period for response to this action is set to expire in 3 (Three) months and 0 (Zero) days from the mailing date of this letter. Failure to respond within the

period for response will result in ABANDOMENT of the application (see 35 U.S.C 133, M.P.E.P 710.02(b)).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shanto M Z Abedin whose telephone number is 571-272-3551. The examiner can normally be reached on M-F from 9:00 AM to 5:30 PM. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser, can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shanto M Z Abedin

Examiner, AU 2136

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

8, 8, 07